

Process Reference Model for Assurance – Goals and Practices September 2010

In the following table, all references to “assurance” are intended to include system and software assurance, information assurance, and cybersecurity in support of the business/mission functions supported by systems and software.

| Goal | Practice List |
|--|---|
| Development – Engineering | |
| DE 1 – Establish assurance requirements | Understand the operating environment and define the operating constraints for mission and information assurance within the environments of system deployment. |
| | Develop customer mission and information assurance requirements. |
| | Define product and product component assurance requirements. |
| | Identify operational concepts and associated scenarios for intended and unintended use and associated assurance considerations. |
| | Identify appropriate controls for integrity and availability of the system to in support of organizational objectives. |
| | Analyze assurance requirements. |
| | Balance assurance needs against cost benefits. |
| | Obtain agreement of risk for assurance level. |
| DE 2 – Create IT solutions with integrated business objectives and assurance | Develop alternative solutions and selection criteria for mission and information assurance. |
| | Architect for assurance. |
| | Design for assurance. |
| | Implement the assurance designs of the product components. |
| | Identify deviations from assurance coding standards. Implement appropriate mitigation to meet defined assurance objectives. |
| DE 3 – Verify and Validate an implementation for assurance | Establish and maintain the environment for assurance validation. |
| | Analyze the results of assurance validation activities. |
| | Establish and maintain verification procedures and criteria for the assurance of selected work products. |
| | Conduct peer reviews according to assurance standards and guidelines. |
| | Analyze the results of assurance verification activities. |

| Goal | Practice List |
|---|--|
| Development - Project | |
| DP – 1 Identify and manage risks due to vulnerabilities throughout the product and system lifecycle | Define/select strategy for management of risk due to vulnerabilities. |
| | Identify assurance defects and effectiveness of corrective actions in other products/systems/operations (and apply to past, present, and future activities). |
| | Determine root causes of mission and assurance defects that are identified during development and operations. |
| | Identify and document risks associated with the identified threats, vulnerabilities, and hazards. |
| | Prioritize risks according to a defined methodology. |
| | Identify mitigation controls and strategies. |
| | Implement corrective action. |
| | Monitor assurance risk. |
| | Identify, analyze and mitigate risks to IT assets that could adversely affect the operation and delivery of services. |
| | |
| DP 2 – Establish and maintain assurance support from the project | Plan for assurance. |
| | Manage for assurance. |
| | Plan for team members with appropriate levels of assurance knowledge. |
| | Establish and maintain the technical infrastructure to support information and mission assurance. |
| | Communicate and coordinate all assurance decisions and recommendations. |
| | Identify, understand, and mitigate risks to the assurance objectives. |
| | Measure effectiveness of project assurance objectives. |
| DP 3 – Protect project and organizational assets | Properly configure and use assurance controls. |
| | Detect and track both internal and external assurance related events. |
| | Respond to incidents according to organizational policy. |

Process Reference Model for Assurance – Goals and Practices September 2010

In the following table, all references to “assurance” are intended to include system and software assurance, information assurance, and cybersecurity in support of the business/mission functions supported by systems and software.

| Goal | Practice List |
|---|---|
| DP 3 – Protect project and organizational assets (continued) | Identify changes to the operational assurance posture of the project and organizational environments and ensure they are addressed in accordance with the assurance objectives. |
| | Plan for continuous availability of project and organizational environment. |
| | Properly maintain process and organizational information labeled with the appropriate assurance classifications. |
| Development – Organization | |
| DO 1 – Establish the assurance resources to achieve key business objectives | Establish and maintain the description of the assurance context and objectives for the organization. |
| | Establish organizational processes to achieve the assurance business objectives. |
| | Establish acceptable deviations and alternatives for assurance processes and policy. |
| | Establish and maintain the technical infrastructure to support information and mission assurance. |
| | Establish and implement an assurance roadmap as part of the plan for the organization. |
| DO2 – Establish the environment to sustain the assurance program within the organization. | Integrate and maintain process assets for assurance across the organization in conjunction with the other system development processes. |
| | Establish and maintain collaborations with external organizations promoting assurance. |
| | Identify, document, and manage IT assets during their lifecycle to ensure sustained assurance. |
| Enterprise - Assurance Support | |
| ES 1 – Establish and maintain organizational culture that supports assurance management, engineering, operations, and support | Coordinate organizational mission and strategy while defining the role of assurance in the engineering and related processes. |
| | Communicate the plan for assurance. |
| | Establish and maintain the strategic assurance training needs of the organization. |

| Goal | Practice List |
|---|--|
| ES 2 – Establish and maintain the ability to support continued delivery of assurance capabilities | Plan for effective delivery of assurance capabilities. |
| | Identify, track, and resolve concerns about effective delivery of assurance capabilities. |
| | Establish, Deliver and Maintain effective delivery of assurance capabilities. |
| ES 3 – Monitor and improve enterprise support to IT assets | Establish, monitor, analyze, and manage an internal control system that ensures the effectiveness and efficiency of operations through assuring mission success of high-value services and the IT assets that support them. |
| | Ensure awareness of and compliance with an established set of relevant internal and external guidelines, standards, practices, policies, regulations, and legislation, and other obligations related to managing IT assets that support the mission. |
| | Ensure the continuity of essential operations of services and related IT assets if a disruption occurs as a result of an incident, disaster, or other disruptive event. |
| | Determine root causes of mission and assurance defects that are identified during development and operations. |
| | Establish processes to identify and analyze events, detect incidents, and determine an appropriate organizational response. |
| | Manage changes to the assurance requirements for services and associated IT assets. |
| | |
| Acquisition and Supplier Management | |
| AM 1 – Select, manage, and use effective suppliers and third party applications based upon their assurance capabilities | Select suppliers based on an evaluation of their ability to meet specified assurance requirements and established criteria. |
| | Document supplier agreements for assurance. |
| | Monitor supplier work processes and work products. |
| | Evaluate supplier deliverables against assurance acceptance criteria. |